JOURNAL OF NUMBER THEORY **24**, 360–372 (1986)

Construction of Some Wreath Products as Galois Groups of Normal Real Extensions of the Rationals

R. Gow

Mathematics Department, University College, Belfield, Dublin 4, Ireland

Communicated by H. Zassenhaus

Received April 11, 1985

Let K be a real algebraic number field. Suppose that G occurs as a Galois group of a normal real extension field of K. Using elementary methods, we show that certain types of split extensions of an elementary abelian 2-group by G also occur as Galois groups of normal real extensions of K. Among other examples, we show that Sylow 2-subgroups of the symmetric and alternating groups of degree 2^n, as well as the Weyl groups of type B_n and D_n, occur as Galois groups of real extensions of the rationals. © 1986 Academic Press, Inc.

In the elementary Galois theory of field extensions, it seems to be very difficult to prove the existence of extensions of the rationals or of cyclotomic extensions of the rationals that have a specified Galois group. Indeed, most realizations of groups as Galois groups over cyclotomic extensions of the rationals $\mathbb{Q}$ employ class field theory or methods of algebraic geometry and complex function theory, together with the Hilbert irreducibility theorem. See, for example, the articles on Galois groups in [1]. The purpose of this paper is to show how an admittedly very restricted family of groups can be realized as Galois groups of normal extension fields of $\mathbb{Q}$ using rather unsophisticated methods of field theory. An important ingredient of our proof is the fact that the normal extension fields which we construct are real fields. We would emphasize that all the groups realized as Galois groups in this paper are already known to occur as a consequence of more general techniques.

We briefly describe our working method. Suppose that K is an algebraic number field and f is an irreducible polynomial of degree n in $K[x]$. Let G be the Galois group of f over K. Define the polynomial g in $K[x]$ by

$$g(x) = f(x^2 + c)$$

0022-314X/86 $3.00

where c is some rational number to be determined later. It is straightforward to see that the Galois group H of g over K is an extension of a normal elementary abelian 2-subgroup N by G. In general, without some knowledge of f, we cannot specify how large N will be, although its order is at most 2^n. Suppose, however, that K is a real algebraic number field, by which we mean that K is contained in the field of real algebraic numbers. Suppose also that all the roots of f are real. By choosing c so that $f(x+c)$ has exactly one negative root, we can prove that the subgroup N described above has order 2^n. Then, by appealing to the Frobenius density theorem, we show that it is possible to make a different choice of c so that all the roots of the corresponding g are now real and the Galois group remains the same. In this way, the process can be repeated. We remark that the Frobenius density theorem is the only part of our proof that is not elementary. Moreover, determination of an appropriate value of c uses the existence of certain primes which would be difficult to find explicitly.

Our main theorems (Theorems 1 and 2 of Sect. 2) are sufficient to realize a Sylow 2-subgroup of the symmetric group S_{2^n} as a Galois group of a normal real extension field of $\mathbb{Q}$. In fact, this group can be realized as the Galois group of an irreducible polynomial of degree 2^n in $\mathbb{Q}[x]$ that has exactly $2m$ real roots for any integer m with $0 \leqslant m \leqslant 2^{n-1}$. Since any 2-group can be embedded into such a Sylow 2-subgroup for sufficiently large n, this construction may be of interest. Similarly, we show that a Sylow 2-subgroup of the alternating group of degree 2^n is a Galois group of a normal real extension of $\mathbb{Q}$. However, it should be recalled that any finite solvable group can be realized as a Galois group over $\mathbb{Q}$, by a theorem of Shafarevich, [8]. Section 3 of this paper contains various examples of Galois groups realized by our technique.

1. Preliminaries

We begin by proving one of the statements made in the introduction. We work with an arbitrary perfect field k of characteristic different from 2.

Lemma 1. *Let f be a nonconstant polynomial of degree n in $k[x]$ and let G denote the Galois group of f over k. Let $g = f(x^2)$ and let H denote the Galois group of g over k. Then there exists a normal elementary abelian 2-subgroup N of H of order dividing 2^n with*

$$H/N \cong G.$$

Proof. Let the roots of g in some splitting field L over k be

$$\alpha_1, -\alpha_1, \ldots, \alpha_n, -\alpha_n.$$

Then L contains the field

$$M = k(\alpha_1^2, \ldots, \alpha_n^2)$$

which is a splitting field for f over k, and hence is a Galois extension of k. Let N be the subgroup of H that fixes all elements of M. By Galois theory, N is normal in H and we have

$$H/N \cong G.$$

Now if σ is in N,

$$\sigma(\alpha_i^2) = \alpha_i^2, \qquad 1 \leqslant i \leqslant n.$$

It follows that

$$\sigma(\alpha_i) = \pm\alpha_i, \qquad 1 \leqslant i \leqslant n.$$

Thus σ^2 fixes all roots α_i and hence is the identity. Therefore, N is an elementary abelian 2-subgroup whose order is clearly at most 2^n. This completes the proof.

Suppose now that T is a subgroup of the finite group G. We will say that T is core-free in G if T contains no proper normal subgroup of G. This is equivalent to saying that the distinct conjugates of T intersect in the trivial subgroup of G. If T is core-free in G and $|G : T| = n$, G is faithfully embedded as a transitive subgroup into the symmetric group S_n by its permutation action on the left cosets of T in G. The following lemma must be well known, but we include a proof for completeness.

LEMMA 2. *Let L be a Galois extension of finite degree of a field k and let G be the Galois group of L over k. Let T be any core-free subgroup of G. Then there exists an irreducible polynomial f in $k[x]$ of degree $n = |G : T|$ whose splitting field is L and a root β of f in L whose fixed point subgroup in G is T.*

Proof. By the normal basis theorem, [3, p. 57], there exists an element α in L such that

$$s_1(\alpha), \ldots, s_m(\alpha)$$

form a basis of L over k, where the s_i are the elements of G. Set

$$\beta = \sum t(\alpha)$$

where the summation extends over all elements t of T. Let

$$1 = u_1, \ldots, u_n$$

be a complete set of left coset representatives for T in G and put

$$\beta_i = u_i(\beta),$$

so that $\beta_1 = \beta$. The n elements $\beta_1, \ldots, \beta_n$ are linearly independent over k and are easily seen to be transitively permuted by G. It can also be checked that the subgroup of G which fixes β is T. Put

$$f = (x - \beta_1) \cdots (x - \beta_n).$$

Then f is invariant under G and its roots are transitively permuted by G. Thus f is irreducible in $k[x]$. Since f splits completely in L, L contains a splitting field M of f over k. Let S be the subgroup of G that fixes all elements of M. Then S is normal in G since M is a Galois extension of k. But as S fixes the root β, it is contained in T. However, T is core-free and thus S is trivial. It follows that $M = L$ and f is the required polynomial.

We end this section with a brief description of the construction of a wreath product. Let G be a finite group having a faithful transitive permutation representation of degree n. If W is any group, G then acts as a group of automorphisms of the direct product

$$U = W \times \cdots \times W$$

of n copies of W by permuting the components of U according to its action on n points. The semidirect product of U by G, where the action of G on U is that just described is called a wreath product of W by G and is denoted here by

$$W \text{ wr } G.$$

While the notation is potentially ambiguous, in that G may have several different transitive permutation representations, we will always specify the permutation action of G when discussing the wreath product. When W is finite, the wreath product just considered has order $|G|\,|W|^n$. Cayley's theorem shows that G has a faithful transitive permutation representation of degree $|G|$. Wreath products constructed using this action of G are called regular wreath products. In all cases that we deal with in this paper, W will have order 2.

2. Proofs of the Main Theorems

We begin by showing how a wreath product $\mathbb{Z}_2$ wr G can be realized as a Galois group whenever G is the Galois group of a polynomial whose roots are all real ($\mathbb{Z}_2$ denotes a cyclic group of order 2).

THEOREM 1. *Let K be a real algebraic number field and let h be a polynomial in $K[x]$ whose roots in some splitting field M over K are all real. Let G be the Galois group of M over K and let T be a core-free subgroup of index n in G. Then there exists a monic irreducible polynomial g in $K[x]$ of degree $2n$ whose Galois group is the wreath product*

$$\mathbb{Z}_2 \text{ wr } G$$

of order $|G|\, 2^n$. The permutation action of G in the wreath product is that determined by its action on the left cosets of T in G.

Proof. Since M is generated over K by the roots of h, M is also a real algebraic number field. By Lemma 2, M is the splitting field of a monic irreducible polynomial f in $K[x]$ of degree n. Moreover, f has a root β whose fixed point subgroup is T. The roots

$$\beta_1 = \beta, \ldots, \beta_n$$

of f must all be real, since M is a real field, and we can assume the notation is chosen so that

$$\beta_1 < \cdots < \beta_n.$$

Now we can find a rational number c with

$$\beta_1 - c < 0, \qquad \beta_i - c > 0, \qquad i > 1.$$

The polynomial $f(x+c)$ in $K[x]$ is irreducible and has n real roots, exactly one of which is negative. We also note that the Galois group of this polynomial is G and the fixed point subgroup of the root $\beta_1 - c$ is T. Thus, we may as well assume that f has exactly one negative root.

We put $g = f(x^2)$, so that g is monic of degree $2n$, and let the roots of g be

$$\alpha_1, -\alpha_1, \ldots, \alpha_n, -\alpha_n$$

in some splitting field L, with $\alpha_i^2 = \beta_i$. Now g has exactly two nonreal roots, α_1 and $-\alpha_1$, which are purely imaginary. Let H denote the Galois group of g over K. By Lemma 1, H contains a normal elementary abelian 2-subgroup N with

$$H/N \cong G.$$

Let t denote the complex conjugation automorphism of L. We have

$$t(\alpha_1) = -\alpha_1, \qquad t(\alpha_i) = \alpha_i, \qquad i > 1.$$

Thus t belongs to N. Now H permutes the roots β_i of f transitively, since f is irreducible. Thus for $i>1$, there exists t_i in H with

$$t_i(\alpha_1^2)=\alpha_i^2.$$

It follows that

$$t_i(\alpha_1)=\pm\alpha_i.$$

We see then that $t_i t t_i^{-1}$ fixes all roots different from $\pm\alpha_i$ and sends α_i to $-\alpha_i$. In this way, we obtain n independent generators for N and therefore N has order 2^n. It is also clear that H permutes the roots of g transitively and therefore g is irreducible.

To complete the proof, we must show that H splits over N. G acts faithfully as a permutation group of degree n. Let G have order m and let the image of G in S_n consist of the permutations

$$\pi_1,\ldots,\pi_m.$$

The permutation action of H on the roots $\alpha_i^2=\beta_i$ is that which is determined by G. Thus if π is any one of the permutations π_j, there exists σ in H with

$$\sigma(\alpha_i^2)=\alpha_{\pi(i)}^2, \qquad 1\leqslant i\leqslant n.$$

It follows then that

$$\sigma(\alpha_i)=\varepsilon_i\alpha_{\pi(i)},$$

where $\varepsilon_i=\pm1$. Since N has order 2^n, there exists a unique element θ in N with

$$\theta(\alpha_{\pi(i)})=\varepsilon_i\alpha_{\pi(i)}, \qquad 1\leqslant i\leqslant n.$$

We see that

$$\theta\sigma(\alpha_i)=\alpha_{\pi(i)}.$$

If we write $\pi'=\theta\sigma$, π' effects the same permutation on the roots $\alpha_1,\ldots,\alpha_n$ as π effects on the roots $\beta_1,\ldots,\beta_n$. Thus if G_1 is the subgroup of H generated by $\pi_1',\ldots,\pi_m'$, we see that G_1 must intersect N trivially and G_1 is isomorphic to G. Therefore G_1 provides the required complement for N and this completes the proof.

To be able to exploit Theorem 1 to obtain repeated wreath products, it is preferable to construct a polynomial g whose roots are also real. In this

case, we want to find an automorphism that takes the place of complex conjugation. Our next theorem shows how this can be done. We need certain ideas from algebraic number theory, which are all well known. However, as we need to introduce new notation, we will briefly review the pertinent theory. A convenient reference for this material is [4].

Let K be an algebraic number field and let g be a nonconstant monic polynomial in $K[x]$. Let L be a splitting field for g over K and let G be the Galois group of g over K. Let R, S be the rings of algebraic integers in K and L, respectively. Given a prime ideal P in R, define the ring of P-local integers $A = R_P$ in K by

$$A = \{\alpha/\beta : \alpha, \beta \in R, \beta \notin P\}.$$

A is a principal ideal domain with quotient field K and has unique maximal ideal PA. We have

$$R/P \cong A/PA \cong k,$$

where k is a finite field of characteristic p, p being the unique prime integer in $P \cap \mathbb{Z}$.

Let $Q_1, \ldots, Q_m$ denote the prime ideals of S lying over P. The Galois group G permutes these ideals transitively. Let Q be a fixed member of the Q_i and let $D = D(Q \mid P)$ be the stabilizer of Q in the permutation action of G on the Q_i. D is called the decomposition group. The finite field $k_1 = S/Q$ is an extension field of k and it inherits a natural action of D as a group of automorphisms over k. If P is unramified in S, D is isomorphic to $\mathrm{Gal}(k_1 : k)$ and is thus cyclic. In this case, let $\phi = \phi(Q \mid P)$ denote a generator of D. The element ϕ is called a Frobenius automorphism and the conjugacy class of ϕ in G is called the Frobenius class.

Let B be the integral closure of A in L. Since the coefficients of g are P-local integers for all but finitely many primes of R, the roots of g lie in B if we avoid the exceptional primes. It is known that the maximal ideals of B have the form Q_iB and they are permuted transitively by G. We also have

$$B/QB \cong S/Q.$$

Thus the decomposition group D acts naturally on B/QB and is isomorphic to $\mathrm{Gal}(B/QB : A/PA) = \mathrm{Gal}(k_1 : k)$ in the unramified case.

Using this notation and the notation in Theorem 1 we can now prove the following theorem.

THEOREM 2. *The polynomial g described in Theorem 1 can be chosen to have the stated Galois group and to have all its roots real.*

Proof. We begin by working with the polynomial g described in the proof of Theorem 1. We recall that if the roots of g in some splitting field L over K are

$$\alpha_1, -\alpha_1, \ldots, \alpha_n, -\alpha_n$$

and H is the Galois group of g over K, the complex conjugation automorphism t in H satisfies

$$t(\alpha_1) = -\alpha_1, \qquad t(\alpha_i) = \alpha_i, \qquad i > 1.$$

Let C be the conjugacy class of H that contains t. By the Frobenius density theorem, [4, p. 134], there exist infinitely many prime ideals P in R which are unramified in S and which have the property that C is the corresponding Frobenius class. Choose such an unramified prime P for which the coefficients of g belong to $A = R_P$. The roots of g then lie in the integral closure, B, of A in L. Let Q be a prime ideal of S that lies over P and is fixed by t. Then $t = \phi(Q \mid P)$ generates the Galois group of $k_1 = S/Q$ over $k = R/P$.

Let $\bar{\alpha}$ denote the image of an element α in B under the canonical map

$$B \to B/QB \cong k_1.$$

Similarly, let $\bar{g}$ denote the image in $k[x]$ of the polynomial g. The roots of $\bar{g}$ in k_1 are $\pm\bar{\alpha}_1, \ldots, \pm\bar{\alpha}_n$, and they are all distinct, since P is unramified. Now in the induced action of t on k_1, we must have

$$t(\bar{\alpha}_1) = -\bar{\alpha}_1, \qquad t(\bar{\alpha}_i) = \bar{\alpha}_i, \qquad i > 1.$$

Thus, since t generates $\mathrm{Gal}(k_1 : k)$, the polynomial $\bar{g}$ is expressible in $k[x]$ as

$$\bar{g} = (x^2 - \bar{\alpha}_1^2) \prod_{i>1} (x - \bar{\alpha}_i)(x + \bar{\alpha}_i),$$

where $\bar{\alpha}_1^2$ is a nonsquare in k and $\bar{\alpha}_i$ is in k, $i > 1$. We see that $\bar{g}$ is a product of an irreducible polynomial of degree 2 and distinct linear factors.

Now let p be the unique prime integer in $P \cap \mathbb{Z}$. Choose an integer r so that the roots of $f(x + rp)$ are all positive, where f is the polynomial assumed in Theorem 1 to have exactly one negative real root. Set

$$g_1 = f(x^2 + rp).$$

Then g_1 is a monic polynomial in $A[x]$ and all its roots are real. Moreover, we have

$$\bar{g}_1 = \bar{g}$$

in $k[x]$. Thus we know that $\bar{g}_1$ is a product of an irreducible polynomial of degree 2 and distinct linear factors. It follows from a theorem of Dedekind, [2, p. 285], that the Galois group of g_1 over K contains an element w which acts as a transposition on the roots of g_1. Since g_1 is a polynomial in x^2, we can assume that the roots of g_1 in some splitting field are

$$\gamma_1, -\gamma_1, \ldots, \gamma_n, -\gamma_n$$

and we can number the roots so that we have

$$w(\gamma_1) = -\gamma_1, \qquad w(\gamma_i) = \gamma_i, \qquad i > 1.$$

But now it can be seen that w takes the role of the complex conjugation automorphism t in our proof of Theorem 1. Thus by imitating that proof, we arrive at the conclusion that the Galois group of g_1 over K is also $\mathbb{Z}_2$ wr G. Since all the roots of g_1 are real, we can replace g by g_1 and thus prove Theorem 2.

Note. Although we want the polynomial g_1 to have real roots and the stated Galois group so that we can repeat the process, we can arrange for g_1 to have the same Galois group and exactly $2m$ real roots for any integer m with $0 \leqslant m \leqslant n$. For, instead of choosing a rational integer r so that the roots of $f(x + rp)$ are all positive, we can find rational integers a, b, with $(b, p) = 1$, so that $f(x + ap/b)$ has exactly m positive roots. Then we define $g_1 = f(x^2 + ap/b)$. We have $\bar{g}_1 = \bar{g}$, since a/b is a p-local integer. The previous argument shows that this new g_1 has the original Galois group and exactly $2m$ real roots.

Recall that if k is a field and V is a $k[G]$-module, V is said to be cyclic if there is some vector v in V such that the vectors $g(v)$, g in G, span V. A module V is cyclic if and only if it is isomorphic to a quotient of the regular module $k[G]$.

COROLLARY 1. *Let K be a real algebraic number field. Suppose that the group G occurs as the Galois group of a normal real extension of K. Let V be any cyclic $GF(2)$-module for G. Then the semi-direct product VG also occurs as the Galois group of some normal real extension field of K.*

Proof. In Theorems 1 and 2, we let T equal the identity subgroup. Then the regular wreath product $H = \mathbb{Z}_2$ wr G of order $|G|\,2^{|G|}$ is realized as the Galois group of a normal real extension of K. Let N denote the normal elementary abelian 2-subgroup of H on which G acts. Considered as a module for G over $GF(2)$, N is clearly isomorphic to the regular module. Thus, as V is cyclic, there exists a G-submodule U of N with

$$N/U \cong V$$

as G-modules. U is a normal subgroup of H and we have

$$H/U \cong VG.$$

Since quotient groups of H are themselves Galois groups of normal real extensions of K, the result follows.

3. Construction of Some Galois Groups

We show how Theorem 2 can be used to realize certain wreath products and related groups as Galois groups of normal real extensions of $\mathbb{Q}$. Define $D_1 = \mathbb{Z}_2$ and consider D_1 as a transitive permutation group of degree 2. Put

$$D_n = \mathbb{Z}_2 \text{ wr } D_{n-1}, \qquad n \geqslant 2,$$

where the wreath product is constructed using the natural transitive permutation action of D_{n-1} of degree 2^{n-1}. It is well known that D_n is isomorphic to a Sylow 2-subgroup of S_{2^n}. Since a given finite group can be embedded into some S_{2^n}, D_n clearly contains an isomorphic copy of any given 2-group, for sufficiently large n.

Theorem 3. *The group D_n is the Galois group of an irreducible polynomial f_n of degree 2^n in $\mathbb{Q}[x]$ whose roots are all real. D_n is also the Galois group of an irreducible polynomial of degree 2^n in $\mathbb{Q}[x]$ that has exactly $2m$ real roots, for any integer m with $0 \leqslant m \leqslant 2^{n-1}$.*

Proof. We proceed by induction on n. For $n = 1$, we can take

$$f_1 = x^2 - 2,$$

whose Galois group over $\mathbb{Q}$ is $\mathbb{Z}_2 = D_1$. Assume now that f_{n-1} has been constructed to have real roots and Galois group D_{n-1}. By Theorem 2, we can construct a polynomial f_n of degree 2^n in $\mathbb{Q}[x]$ whose roots are all real and whose Galois group is $\mathbb{Z}_2 \text{ wr } D_{n-1} = D_n$. Following the note after Theorem 2, we can modify our construction of f_n so that it has exactly $2m$ real roots and retains the same Galois group. This completes the proof.

Example. Although not constructed entirely using the ideas of Theorem 2, we find that

$$f = [(x^2 - 10)^2 - 7]^2 - 2$$

has Galois group D_3 of order 128, and all the roots of f are real.

A modification of this construction yields the following result.

THEOREM 4. *A Sylow 2-subgroup of the alternating group A_{2^n} of degree 2^n is the Galois group of a normal real extension of $\mathbb{Q}$.*

Proof. We have realized a Sylow 2-subgroup D_n of S_{2^n} as the Galois group of a rational polynomial f_n whose roots $\pm\alpha_i$, $1 \leqslant i \leqslant 2^{n-1}$, are all real. D_n is a semi-direct product $N_n D_{n-1}$, where N_n is elementary abelian. The action of an element s of N_n on the roots has the form

$$s(\alpha_i) = \varepsilon_i \alpha_i, \qquad 1 \leqslant i \leqslant 2^{n-1},$$

where $\varepsilon_i = \pm 1$. Consider the subgroup M_n of N_n consisting of all those s in N_n for which we have

$$\prod \varepsilon_i = 1.$$

M_n is normal in D_n and has index 2 in N_n. Moreover, considered as a $GF(2)$-module for D_{n-1}, M_n is easily seen to be cyclic. Since it is known that a Sylow 2-subgroup of A_{2^n} is isomorphic to the semi-direct product $M_n D_{n-1}$, the result follows from Corollary 1.

There is another family of 2-groups that we can realize as Galois groups by our technique. Let $GL(n, 2)$ denote the group of invertible $n \times n$ matrices with coefficients in $GF(2)$. Let E_n denote a Sylow 2-subgroup of $GL(n, 2)$. If V_n denotes a vector space of dimension n over $GF(2)$, E_n has a natural action on V_n and it is known that E_{n+1} is isomorphic to the semi-direct product $V_n E_n$. It is also elementary to check that V_n is a cyclic E_n-module. Since E_2 is cyclic of order 2, it is certainly realized as a Galois group of a normal real extension of $\mathbb{Q}$. Proceeding by induction on n, and using Corollary 1, we have the next result.

THEOREM 5. *A Sylow 2-subgroup of $GL(n, 2)$ is a Galois group of a normal real extension of $\mathbb{Q}$.*

Finally, we consider some examples involving the symmetric group S_n. In [6], Schur proves that S_n is the Galois group of the Laguerre polynomial L_n of degree n defined by

$$L_n = e^x \frac{d^n}{dx^n}(x^n e^{-x}).$$

Since the roots of L_n are real (and positive), we see that S_n is the Galois group of a normal real extension of $\mathbb{Q}$. If we form the wreath product $W_n = \mathbb{Z}_2 \operatorname{wr} S_n$, where S_n permutes n copies of $\mathbb{Z}_2$, it follows from Theorem 2 that W_n is the Galois group of a normal real extension of $\mathbb{Q}$. W_n

is isomorphic to the Weyl group of a simple Lie algebra of type B_n (or type C_n).

It is not hard to show that if U_n denotes a Weyl group of type D_n, U_n is also a Galois group of a normal real extension of $\mathbb{Q}$. This can be proved in the following manner. U_n is a subgroup of index 2 in W_n, being the intersection of W_n with A_{2n}, when W_n is considered as a permutation group of degree $2n$. We can write W_n as a semi-direct product N_nS_n, where N_n is elementary abelian of order 2^n. Then U_n is expressible as a semi-direct product $U_n = M_nS_n$, where M_n is defined analogously to the M_n in Theorem 4, with M_n having index 2 in N_n. Again, it is straightforward to prove that M_n is a cyclic $GF(2)$-module for S_n. Therefore, we can sum up this discussion as follows.

THEOREM 6. *The Weyl groups of type A_n, B_n, and D_n are all Galois groups of normal real extensions of $\mathbb{Q}$.*

We note that all Weyl groups corresponding to simple Lie algebras are known to occur as Galois groups over $\mathbb{Q}$ (see, for example, the "Queries" page of *Amer. Math. Soc. Notices* February 1974). It would be interesting to know whether the Weyl groups of the exceptional simple Lie algebras can be realized as Galois groups of real extensions of $\mathbb{Q}$.

We also mention, without proof, that work of Schur in [7] enables us to prove in a straightforward manner that the Galois group of the Hermite polynomial H_{4n} defined by

$$H_{4n} = e^{x^2/2} \frac{d^{4n}}{dx^{4n}} (e^{-x^2/2})$$

is isomorphic to $\mathbb{Z}_2$ wr S_{2n}. Since H_{4n} has real roots, this provides a simple concrete example of a polynomial realizing the Weyl group of type B_{2n} as a Galois group of a real extension of $\mathbb{Q}$. We do not know if this holds for H_{4n+2}.

It should be remarked that the groups we have realized as Galois groups over $\mathbb{Q}$ are split extensions of normal abelian subgroups by groups that also occur as Galois groups over $\mathbb{Q}$. Such groups are known to occur as Galois groups over $\mathbb{Q}$ as a consequence of an embedding theorem of Scholz [5]. We also note that in [9], Odoni realizes a Sylow 2-subgroup D_n of S_{2^n} as a Galois group over $\mathbb{Q}$. He shows that D_n is the Galois group of the polynomial f_n defined iteratively by $f_1 = x^2 - x + 1$, $f_n = f_1(f_{n-1})$, $n > 1$.

ACKNOWLEDGMENTS

This work was written while the author was a Visiting Associate Professor at the University of Wisconsin, Madison during 1984-5. I wish to thank the members of the Mathematics Department in Madison for their hospitality during this time.

REFERENCES

1. M. ASCHBACHER ET AL. (Eds.), "Proceedings Rutgers Group Theory Year 1983–1984," Cambridge Univ. Press, New York/Cambridge, 1984.
2. L. C. GROVE, "Algebra," Academic Press, New York/London, 1983.
3. N. JACOBSON, "Lectures in Abstract Algebra," Vol. III, Van Nostrand–Reinhold, New York, 1964.
4. G. J. JANUSZ, "Algebraic Number Fields," Academic Press, New York/London, 1973.
5. A. SCHOLZ, Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe, *Math. Z.* **30** (1929), 332–356.
6. I. SCHUR, Gleichungen ohne Affekt, *in* "Gesammelte Abhandlungen," Band III, pp. 191–197, Springer-Verlag, Berlin/Heidelberg/New York, 1973.
7. I. SCHUR, Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome, *in* "Gesammelte Abhandlungen," Band III, pp. 227–233, Springer-Verlag, Berlin/Heidelberg/New York, 1973.
8. I. R. SHAFAREVICH, Construction of fields of algebraic numbers with given solvable Galois group, *Transl. Amer. Math. Soc. (2)* **4** (1956), 185–237.
9. R. W. K. ODONI, On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$, *J. London Math. Soc. (2)* **32** (1985), 1–11.